CAPACIDADES TECNICAS LEGALES Y DE GESTION PARA EQUIPOS BLUETEAM Y REDTEAM

ALEXANDER PEREZ NOVOA

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM

Director:
M. SC. JOHN FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD.
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2021

TABLA DE CONTENIDO

RESUMEN

Se buscar presentar por medio de este documento un resumen de las diferentes etapas trabajadas durante el seminario especializado red team & blue team, donde se buscó plantear diferentes escenarios en los cuales un especialista de seguridad debe desarrollar al máximo sus conocimientos capacidades técnicas así como demostrar la experiencia para llevar a cabo, lograr identificar así como para buscar soluciones que conlleven a la solución de diferentes escenarios donde involucran sistemas operativos, aplicaciones y las muy diferentes vulnerabilidades y amenazas que se puedan presentar en este tipo de sistemas.

ABSTRACT

Through this document, the aim is to present a summary of the different stages worked during the course of the specialized seminar red team & blue team, where it was sought to propose different scenarios in which a security specialist must develop their knowledge and technical capabilities to the maximum in order to demonstrate the experience to carry out a task, to identify as well as to look for solutions that entail a solution of different scenarios involving operating systems, applications and the very different vulnerabilities and threats that can occur in this type of system.

GLOSARIO

BLUETEAM: Se trata de un grupo de especialistas en seguridad que rastrean ciberincidentes y realizan análisis de los sistemas para garantizar la seguridad, identificar posibles fallos, verificar la efectividad de cada medida y que asegurar que todas las medidas sean efectivas tras su implantación

REDTEAM: Los Red Teams emulan a los atacantes, utilizando sus mismas herramientas o similares, explotando las vulnerabilidades de seguridad de los sistemas y/o aplicaciones (exploits), técnicas de pivoting (saltar de una máquina a otra) y objetivos (sistemas y/o aplicaciones) de la organización

AMENAZA: toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información

INFORMACION: Activo intangible en el cual se manejan identificaciones, datos personales, cuentas, datos empresariales y corporativos, propiedad intelectual, conocimiento comercial, formulación de productos o servicios.

VULNERABILIDAD: es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma.

MAQUINA VIRTUAL: Entorno de virtualización mediante el uso de diferentes herramientas las cuales permiten a partir de un solo dispositivo físico contar con particiones virtuales en las cuales pueden convivir diferentes sistemas operativos, de este modo se pueden realizar pruebas de vulnerabilidad a aplicaciones y archivos.

EXPLOIT: Uso de la vulnerabilidad en una aplicación, sistema informático, archivo, la cual se aprovecha de manera no autorizada.

METASPLOIT: Metasploit Framework es una plataforma modular de pruebas de penetración basada en Ruby que le permite escribir, probar y ejecutar código de explotación. Metasploit Framework contiene un conjunto de herramientas que puede utilizar para probar vulnerabilidades de seguridad, enumerar redes, ejecutar ataques y evadir la detección

METERPRETER: Meterpreter es un payload de Metasploit que proporciona un shell interactivo desde el cual un atacante puede explorar la máquina objetivo y ejecutar código.

INTRODUCCIÓN

El siguiente trabajo está enfocado en buscar e identificar las principals causas y consecuencias que se pueden presenter ante un evento o incidente de seguridad.

Actualmente las diferentes organizaciones encuentran que la información y la seguridad de la misma es uno de los activos más importantes, razón por la cual se deben evaluar los diferentes riesgos a los cuales está expuesta y comprometida; de allí que sea tan necesario actualmente protegerla y brindarle un adecuado aseguramiento.

Se busca fortalecer los entornos de seguridad por medio de pruebas o laboratorios controlados o de diferentes herramientas para encontrar vacios o huecos en la seguridad y asi salvagurdar o mejorar la proteccion para poder tener citerios y optar por medidas de seguridad mas confiables y dinamicas.

En el entorno actual se presentan múltiples fuentes de información confiable para contrarrestar las amenazas o ataques que se presentan a diario a nivel global; estas medidas se deben estar actualizando ya que dia a dia tambien se presentan nuevas amenazas y vulnerabilidades. Los sistemas informáticos son expuestos en gran mayoría a fuentes de amenaza nuevos que se debe estar atento a mitigar o corregir la vulnerabilidad.

DEFINICIÓN DEL PROBLEMA

Las diferentes empresas u organizaciones actualmente se encuentran expuestas a diferentes amenazas y vulnerabilidades en sus servicios informáticos esto se encuentra en constante crecimiento y actualización debido al desarrollo constante de software y a la evolución en las diferentes tecnologías de comunicación razón por la cual se deben buscar estrategias que permitan identificar los posibles riesgos y vulnerabilidades para evitar que sea expuesta la información o los sistemas donde se alojen la misma; se busca al final salvaguardar la información y protegerse de los riesgos actuales externos.

JUSTIFICACION

Actualmente la información es el activo más valioso activo del cual depende el buen funcionamiento de una organización. Mantener su integridad, confidencialidad y disponibilidad es esencial. Por esa razón, desde tiempos anteriores las organizaciones han puesto los medios necesarios para evitar el robo y manipulación de sus datos confidenciales. Desafortunadamente, es relativamente sencillo por las diferentes amenazas y vulnerabilidades tener acceso a las herramientas que permiten a personas no autorizadas llegar hasta la información protegida, con poco esfuerzo y conocimientos, causando graves consecuencias para una organización ya sea desde el tipo de credibilidad como del tipo legal

Para salvaguardar la información el área de seguridad informática de una compañía debe contar con criterios como conocimientos y practica para llevar a un buen nivel de protección la organización y así evitar posibles ataques e infiltraciones de seguridad.

1. OBJETIVOS

1.1 Objetivo General

Identificar y conceptualizar las diferentes temáticas prácticas y conceptuales logrando alcanzar un desarrollando y su vez destrezas para determinar posibles amenazas como vulnerabilidades, para también llegar a determinar futuras contenciones o mejoras en la seguridad.

1.2 Objetivos específicos

- Identificar los diferentes aspectos legales involucrados referentes a la seguridad de la información en Colombia
- Realizar y ejecutar un entorno de prueba virtual para detallar y hacer uso de las diferentes herramientas propuestas.
- Saber diferenciar los diferentes contextos involucrados en las temáticas vistas como distinguir las vulnerabilidades, medidas de mitigación
- Conocer e identificar en ambientes controlados fallos de seguridad específicos que se manipular y detallar en un ambiente de pruebas.
- Documentar los pasos específicos para llegar a encontrar el fallo o fallos de seguridad en los entornos de prueba planteados
- Corregir y mitigar posibles vulnerabilidades mediante Harding del sistema propuesto e investigado

2. DESARROLLO DEL INFORME

2.1 Acciones referente a conceptos equipos de seguridad

Dentro del margen legal en Colombia sobre delitos informáticos y protección de datos personales redacte con sus propias palabras que legislación "leyes, decretos" existen actualmente y las características principales de cada ley.

De las principales y actualizadas hago referencia a 1 específicamente:

Ley 1273 de 2009 el cual es relacionado a:

Capitulo 1ro: hace relación a la Protección de la información y de los datos y sus puntos principales:

Artículo 269a. Acceso abusivo a un sistema informático
El que acceda a un recurso informático asegurado sin autorización incurrirá en pena de cárcel o multa en dinero

Artículo 269b. Obstaculización ilegítima de sistema informático o red de telecomunicación
El que impida o detenga el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de cárcel o multa en dinero

Artículo 269c. Interceptación de datos informáticos
El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de cárcel.

Artículo 269d. Daño informático
El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de cárcel o multa

Artículo 269e. Uso de software malicioso
El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u

otros programas de computación de efectos dañinos, incurrirá en pena de cárcel o multa.

Artículo 269f. Violación de datos personales
El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de cárcel o multa

Artículo 269g. Suplantación de sitios web para capturar datos personales
El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de cárcel o en multa. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. la pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito

Capitulo 2do: De las atentados informáticos y otras infracciones

Artículo 2691. Hurto por medios informáticos y semejantes
El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269j: transferencia no consentida de activos
El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito.

En el mundo de la ciberseguridad existen procesos definidos para poder ejecutar de forma organizada lo que se conoce como pruebas de penetración o pentesting; estas son las etapas del pentesting,

Etapas de un pentesting

- Contacto: es la fase inicial donde se acuerdan los alcances y en que va a consistir específicamente el pentest, definiendo los objetivos y cuáles son los servicios más críticos a revisar; así como para obtener la autorización por escrito de los acuerdos y limitantes.

  La herramienta que se puede utilizar para esta fase seria cualquier editor de texto o programa para definir cronogramas como Project o hoja de calculo

- Fase de recolección de información: es la fase del pentest donde se dedicara tiempo para obtener la mayor información posible del cliente esto mediante arañas o de scanners para tener una idea de los sistemas; también se realiza ingeniería social enfocada a empleados asi como a sus redes sociales.

  La herramienta que se puede utilizar para esta fase, seria Web Crawler una araña Web basada en Python, orientado a ayudar en las tareas de test de penetración

- Fase de modelado de amenaza: es la fase en la que se debe analizar la información recolectada y pensar como si fuera atacante como utilizarla asi como buscar la estrategia de penetración. Esto se debe definir con detalle para saber como poder llegar a los objetivos planteados, en resumen plantearse la estrategia.

  La herramienta que se puede utilizar para esta fase, seria Tutamen donde se pueden modelar las amenazas.

- Fase de análisis de vulnerabilidades: es la fase en la que como su nombre lo indica se deben identificar de forma proactiva las vulnerabilidades. En esta fase es cuando se valida la habilidad del pentester para seleccionar y utilizar correctamente las herramientas a su disposición y asi conseguir objetivos establecidos.

  La herramienta que se puede utilizar para esta fase, seria Nessus

- Fase de explotación: es la fase donde se consigue acceso a los sistemas objetivo del test de penetración planteado, para esto se ejecutaran exploits contra las vulnerabilidades identificadas en las fases anteriores o se utilizaran credenciales obtenidas para ganar acceso a los sistemas

  La herramienta que se puede utilizar para esta fase, Metasploit

- Fase de post-explotacion: es la fase donde luego de haber intentado la explotación inicial se busca recavar sobre otras vulnerabilidades o de realizar pasos laterales con credenciales o con accesos conseguidos.

  La herramienta que se puede utilizar para esta fase, podría ser un Backdoor o un Keylogger

- Fase de informe: es la fase donde se presentan los resultados de lo obtenido, se pueden presentar 2 tipos de informes uno técnico para los administradores de la infraestructura y el sistema y otro informe ejecutivo para los directivos.

Las herramientas de ciberseguridad son de vital importancia, además que existe un gran abanico de posibilidades de herramientas existentes y software especializado para desarrollar herramientas propias. se muestran las siguientes que se pueden utilizar:

Herramientas

- **Metasploit**: es una herramienta para desarrollar y ejecutar un ataque contra una vulnerabilidad encontrada en una máquina remota, permite también realizar auditorías de seguridad, asi como probar y desarrollar sus propios exploits. Un metasploit puede realizar muchas cosas entre las cuales puede escanear y recopilar toda la información de una máquina, identificar y explotar vulnerabilidades, realizar escalamiento de privilegios y robo de datos, instalación de una puerta trasera, fuzzing asi como eliminación de registros y trazas

- **Nmap:** es una herramienta de código abierto para escaneo de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP "crudos" en formas originales para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando así como otras muchas características. Tambien puede testear la seguridad de diversos sistemas informáticos, descubriendo servicios u ordenadores conectados a una red para intentar conseguir información sobre ellos y ver algunas posibles vulnerabilidades o puntos de entrada.

- **OpenVas:** inicialmente denominado GNessUs, es una suite de software, que ofrece un marco de trabajo para integrar servicios y herramientas especializadas en el escaneo y gestión de vulnerabilidades de seguridad de sistemas informáticos. A través de las interfaces se interactúa con dos servicios: OpenVAS Manager y OpenVAS Scanner. El gestor es el servicio que

lleva a cabo tareas como el filtrado o clasificación de los resultados del análisis, control de las bases de datos que contienen la configuración o los resultados de la exploración y la administración de los usuarios, incluyendo grupos y roles. Por su lado, el escáner ejecuta las denominadas NVT (Network Vulnerability Tests), es decir, las pruebas de vulnerabilidades de red, conformadas por rutinas que comprueban la presencia de un problema de seguridad específico conocido o potencial en los sistemas. Las NVT se agrupan en familias de pruebas similares, por lo que la selección de las familias y/o NVT individuales es parte de la configuración de escaneo

Servicios en línea

- **ExploitDB:** es un servicio en línea que es utilizado cuando se encuentran vulnerabilidades por medio de herramientas como OpenVas y se necesita de un mecanismo que permita explotarla, es ExploitDB una suite que centraliza todos los exploits que se pueden utilizar para explotar esa vulnerabilidad, haciendo el trabajo mas accequible. Entrando al sitio web de la herramienta https://www.exploit-db.com/ lo primero que se encuentra es el buscador de vulnerabilidades el cual permite colocar filtros como el tipo (local, remoto, webapps), plataforma (Android, ASP etc.), Autor, Puerto y tag (Console, Cross Site Scripting) al encontrar la vulnerabilidad podemos abrirla y descargar el exploit, inclusive indica si exploit-db ya verificó si el exploit funciona o no.

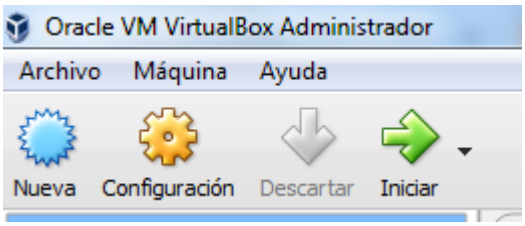
- **CVE:** Es un servicio que se encarga de recopilar las fallas de seguridad en los sistemas informáticos, permitiendo priorizarlos y solucionarlos lo más pronto posible, almacena y organiza las fallas de una manera estándar ayudando a profesionales y organizaciones encontrar la información más rápido, esta herramienta no aporta datos técnicos o como se debe solucionar falla de seguridad (impacto, solución etc.), para esto se deben utilizar otro tipo de herramientas, CVE asigna a cada falla un número de identificación, una característica es que cualquier usuario o empresa podría reportar un fallo de seguridad, CVE clasifica la vulnerabilidad en una escala de 0 a 10. El número CVE asignado a las fallas de seguridad es de la siguiente manera CVEYYYY-NNNNN45

Se creo un “banco de trabajo” para tener el Escenario sobre el cual se probaran los puntos tecnicos

El escenario es el siguiente:

Paso A: Descargar la herramienta virtualizadora “VirtualBox” en su última versión.

Figura 2.1 Instalación de VirtualBox



Paso B: Una vez se realice apertura del foro para el desarrollo de la actividad se procederá a compartir enlace de descarga de lo requerido para el montaje del banco de trabajo, las imágenes en formato .OVA las cuales se encuentran ya preconfiguradas para ser utilizadas en las actividades de carácter técnico. En las imágenes .OVA existe: Un windows 7 X86, un windows 7 X64, un Kali Linux.

Figura 2.2 Descarga de medios

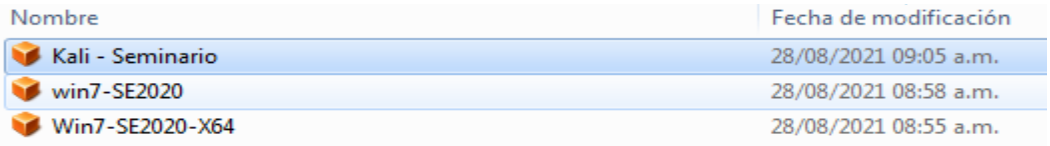


Figura 2.3 Importando Kali

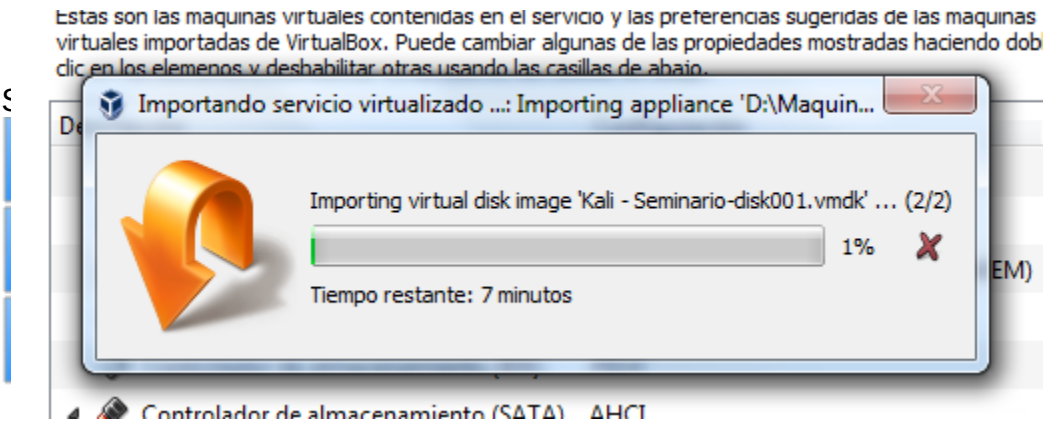


Figura 2.4 Inicio de máquinas virtuales

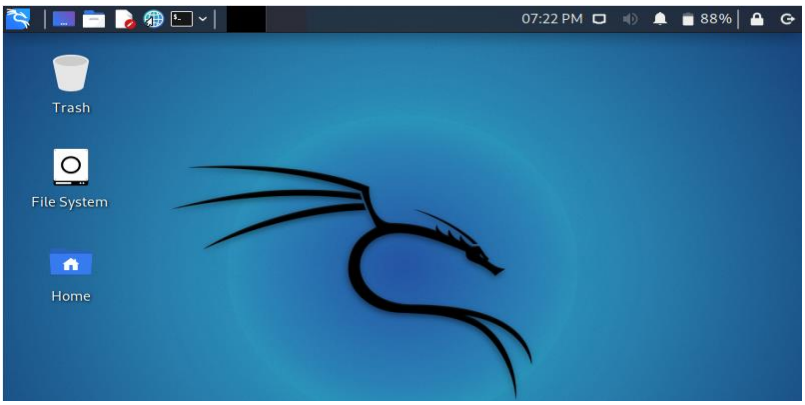


Figura 2.5 Windows 7 - 1

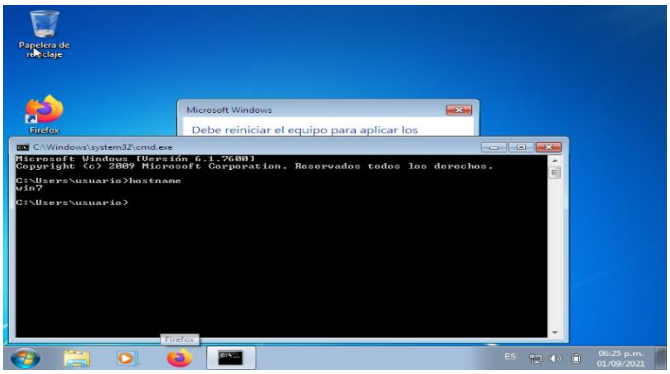
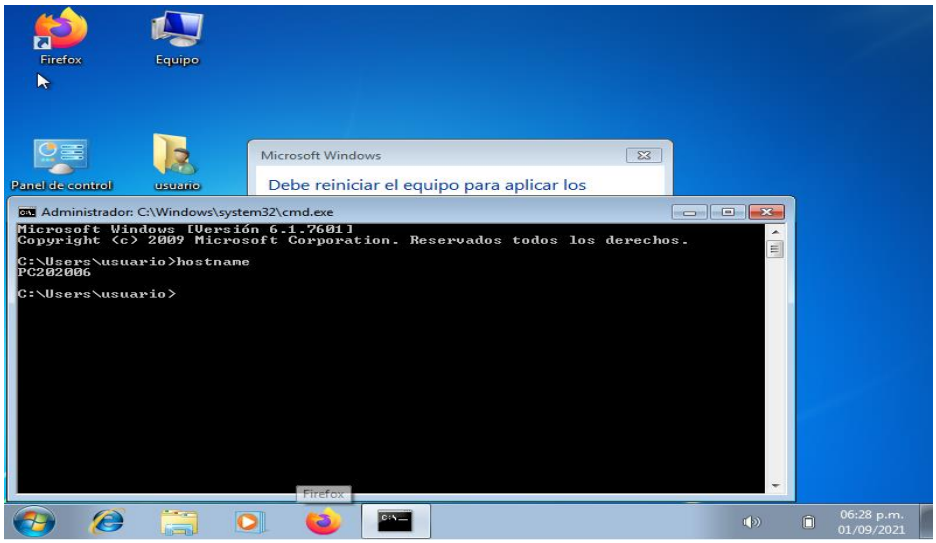


Figura 2.6 Windows 7 - 2



Paso C: Debe validar que exista comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux, recuerde por favor no encender las tres máquinas al tiempo ya que puede colapsar los recursos hardware de su equipo host, encienda primero una máquina Windows y posterior a ello encienda la máquina Kali Linux.

Figura 2.7 Asignación y toma de IPs máquinas virtuales Kali192.168.0.26

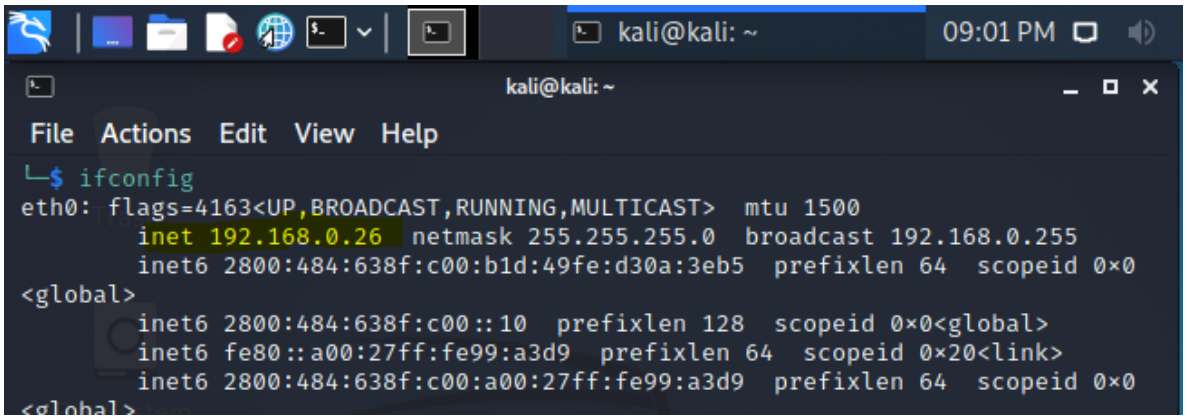


Figura 2.8 Pc202006 Toma IP

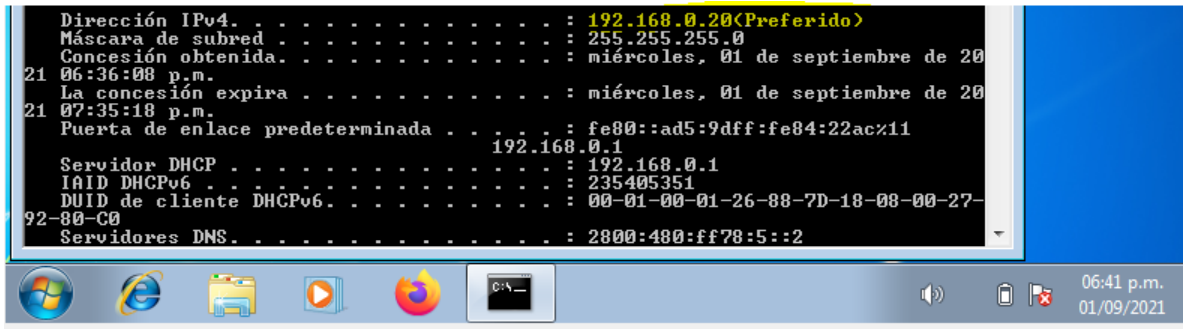


Figura 2.9 Win7 Toma IP

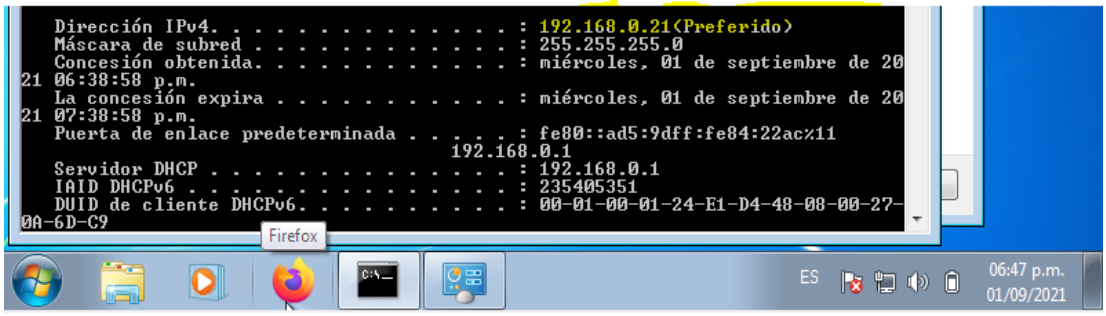


Figura 2.10 Comunicación desde el Kali a las Windows

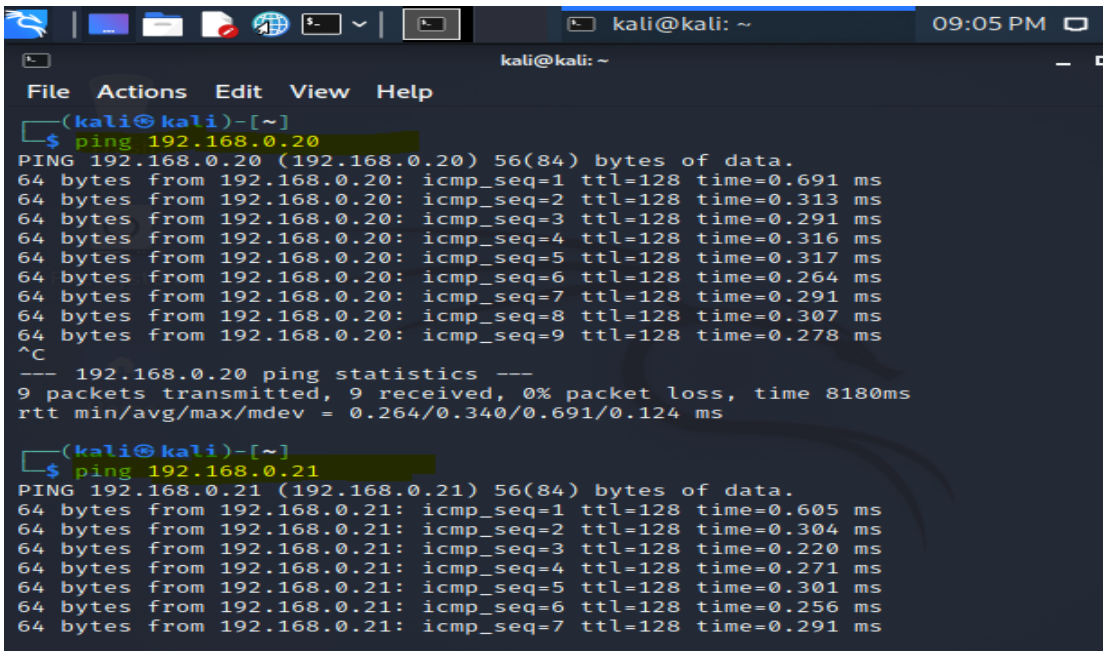
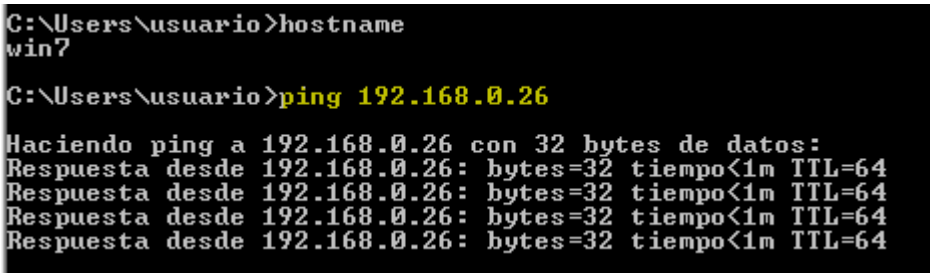
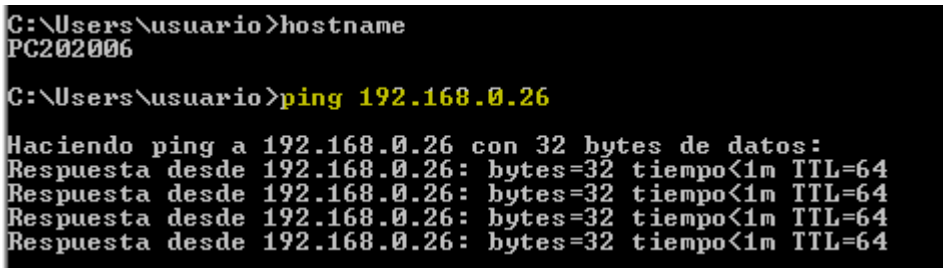


Figura 2.11 Comunicación desde las maquinas Windows al Kali





2.2 Acciones de actuación ética y legal

Dentro de que se logra evidenciar hay procesos ilegales y no éticos que se esté estipulando en dicho acuerdo?

Se realiza lectura a los documentos indicados y según criterio propio creo que lo siguiente no aplica como ético para lo referente a las cláusulas de confidencialidad:

Respecto a las consideraciones

- Punto 2: se habla que la información fue obtenida legalmente por parte de WhiteHouse Security > esto no es comprobable en el momento de la firma del acuerdo por parte de la parte receptora

Respecto a las clausulas

- Primera Objeto: se refieren a la confidencialidad de la parte receptora > en este punto se habla de que también deben guardar confidencialidad a procesos ilegales dentro de WhiteHouse Security no es punto ético y va en contra de los principios que deberían tener una organización
- Segunda definición de información confidencial > en este punto se habla de datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos temas e información no éticos y que una compañía no debería tener por más que sea una empresa de ciberseguridad.
- Tercera origen de la información confidencial > no es claro el texto pero por lo que se entiende tampoco aplicarían temas que se definen como creaciones de intelecto de los documentos sin importar que se requiera definir el carácter confidencial.
- Cuarto obligaciones de la parte receptora > Puntos 3 y 4 donde hacen referencia a No denunciar y abstenerse de denunciar actividades sospechosas e información ilegal; actividades no éticas dentro de una organización la cual va en contra de los principios organizacionales.

- Cuarto obligaciones de la parte receptora > Puntos 7, 8 y 9 donde se habla de responder por el mal uso que le den los representantes de WhiteHouse a la información confidencial y de responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento; un puede ser que un estudiante y/o cualquier persona en una organización tenga que responder por las malas prácticas de la organización.

- Octava solución de controversias > donde se habla de que en caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security; este tipo de acuerdos no se ven lo más legales para que un estudiante tenga que responder por las prácticas ilegales de la organización.

Si la respuesta es afirmativa y usted encontró algún proceso ilegal en el anexo 3 - Acuerdo deberá mencionar que artículos de la ley 1273 se podrían vulnerar en dicho acuerdo y especificar porqué vulnera artículos de la ley 1273.

Si se encuentran procesos ilegales en el acuerdo anexo 3 los cuales si vulneran la ley 1273 como los siguientes:

- Artículo 269F. Violacion de datos personales > lo vulnera cuando se hace referencia a que sacan provecho propio de la información que llegaran a tener por medios no éticos.
- Artículo 269H. Circunstancias de agravación punitiva > ya que se indica que aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este genere ganancias y con la información, revele o de al conocer el contenido de la información en perjuicio de otro y tambien obteniendo provecho para si mismo o para un tercero
- Artículo 2691. Hurto Por Medios Informáticos Y Semejantes > este es vulnerado ya que como se indca en el acuerdo en algún momento sustrain información de chuzadas interceptando información de una manera no concentuada.

¿Existiendo procesos poco confiables en el anexo 3 – Acuerdo? usted como experto en ciberseguridad aplicaría a este trabajo en The WhiteHouse, donde la organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio? Debe argumentar su respuesta ya sea

afirmativa o negativa y tener en cuenta en la argumentación lo que se dispone en COPNIA en su código de ética para ingenieros.

El salario es llamativo, pero de mi parte no aceptaría la propuesta laboral inicialmente por mi ética moral y por lo que me han inculcado desde niño respecto a valores y luego por la ética profesional que conlleva según el código de COPNIA:

- El ejercicio profesional de la Ingeniería en todas sus ramas, de sus profesiones afines y sus respectivas profesiones auxiliares, debe ser guiado por criterios, conceptos y elevados fines, que propendan a enaltecerlo; por lo tanto deberá estar ajustado a las disposiciones de las siguientes normas que constituyen su Código de Ética Profesional.
- Artículo 35. Deberes de los profesionales para con la dignidad de sus profesiones. Son deberes de los profesionales de quienes trata este Código para con la dignidad de sus profesiones: a) Sentencia C-570 de 2004, Corte Constitucional. Inexequible. Contribuir con su conducta profesional y con todos los medios a su alcance para que en el consenso público se preserve un exacto concepto de estas profesiones, de su dignidad y del alto respeto que merecen; b) Respetar y hacer respetar todas las disposiciones legales y reglamentaras que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones; c) Velar por el buen prestigio de estas profesiones; 11 Código de Ética d) Sus medios de propaganda deberán ajustarse a las reglas de la prudencia y al decoro profesional, sin hacer uso de medios de publicidad con avisos exagerados que den lugar a equívocos sobre su especialidad o idoneidad profesional.

Adicional a lo anterior tambien se afectaría y se entienden por faltas gravísimas dentro del codigo:

Se refiere a este texto en detalle según el código; no se cambia para dar claridad a lo que se quiere indicar

- Se constituyen en causal de cancelación de la matrícula profesional, sin requerir la calificación que de ellas haga el Consejo respectivo, las siguientes faltas: 17 Código de Ética a) Derivar, de manera directa o por interpuesta persona, indebido o fraudulento provecho patrimonial en ejercicio de la profesión, con consecuencias graves para la parte afectada; b) Obstaculizar, en forma grave, las investigaciones que realice el Consejo Profesional de Ingeniería respectivo; c) Abandono injustificado de los encargos o compromisos profesionales, cuando con tal conducta causen grave detrimento al patrimonio económico del cliente o se afecte, de la misma forma, el patrimonio público; d) La utilización fraudulenta de las hojas de vida de sus colegas para

participar en concursos, licitaciones públicas, lo mismo que para suscribir los respectivos contratos; e) Incurrir en algún delito que atente contra sus clientes, colegas o autoridades de la República, siempre y cuando la conducta punible comprenda el ejercicio de la ingeniería o de alguna de sus profesiones auxiliares; f) Cualquier violación gravísima, según el criterio del Consejo respectivo, del régimen de deberes, obligaciones y prohibiciones que establecen el Código Ética y la presente ley.

Deberá buscar la noticia del caso "OPERACIÓN ANDROMEDA BUGGLY" en la ciudad de Bogotá, y redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar.

Inicialmente BUGGLY se dio a conocer como un sitio donde se apoyaban y buscaban generar capacitaciones y brindar información de ciberseguridad, para luego convertirse en una especie de club o comunidad de expertos o conocedores en temas de seguridad informática brindando su servicios y tambien disfrutando de un modo light este proceso.

Luego revisando en mas detalle se encontró que todo era parte de la Operación Andrómeda, una fachada de la Central de Inteligencia Técnica del Ejército Nacional. Esto se financiaba de fondos de los gastos reservados,. Su misión, según la orden de operaciones que le dio origen, era adquirir conocimientos de informática del hacking ético.

Esta fachada exigía que Buggly se dedicara, especialmente, a atraer miembros a la comunidad de hacking ético y a obtener sus conocimientos. Por eso brindaban fiestas y otoegaban generosidad a los integrantes que llegaban: esto servía para saber qué alcance o habilidad específica tenian algunos hackers y luego asi reclutarlos.

Luego de las investigaciones por parte de la autoridades se encontró que se estaban realizan operaciones no éticas de infiltraciones y toma de datos por medio de chuzadas, software intrusivo, interceptación de comunicaciones y software malicioso.
Según lo leído e investigado se vulneraron varios códigos éticos asi como se infringieron varias leyes cibernéticas que están en la ley 1273 sobre todo porque la información es confidencial si no se tiene el visto bueno para obtenerla; para lo que ocurre en este evento es claro que el fin no justifica los medios y mas si es información relevante o que debe ser autorizada su uso o búsqueda por una ley clara.

2.3 Acciones de pruebas de intrusión

Las herramientas de software para un escenario enfocado a Redteam con las evidencias utilizadas.

Herramientas utilizadas según pasos de pentesting:

- Etapa de recolección de información > La información inicial con la que se cuenta es que hay una máquina donde se está generando la fuga de información y en esta maquina tienen instalada una aplicación llamada rejetto v. 2.3 bajo un sistema operativo windows 7 con arquitectura X64

- Etapa de fase de modelado > Se busca plantear la estrategia para encontrar las mejores opciones y asi modelar las amenazas

- Etapa de análisis de vulnerabilidades > Se encuentra que la herramienta que se indica en el Anexo 4 Rejetto V 2.3 tiene vulnerabilidades referentes a Ejecución remota de comandos como se indica en las imágenes y según su calificación

Figura 2.3.1 Vulnerabilidad

#	ID CVE	ID de CWE	# de exploits	Tipo (s) de vulnerabilidad	Fecha de publicación	Fecha de actualización	Puntaje	Nivel de acceso ganado	Acceso	Complejidad	Autenticación	Conf.	Integ.	Aprovechar.
1	CVE-2020-13432	120			2020-06-08	2021-04-06	5,0	Ninguno	Remoto	Bajo	No requerido	Ninguno	Ninguno	Parcial
rejetto HFS (también conocido como HTTP File Server) v2.3m Build # 300, cuando se utilizan archivos o carpetas virtuales, permite a los atacantes remotos desencadenar una infracción de acceso de escritura de puntero no válido a través de solicitudes HTTP simultáneas con un URI largo o encabezados HTTP largos.														
2	CVE-2014-7226	94	1	Código ejecutivo	2014-10-10	2014-10-10	7.5	Ninguno	Remoto	Bajo	No requerido	Parcial	Parcial	Parcial
La función de comentario de archivo en Rejetto HTTP File Server (hfs) 2.3cy versiones anteriores permite a los atacantes remotos ejecutar código arbitrario cargando un archivo con ciertas secuencias de bytes UTF-8 no válidas que se interpretan como macro símbolos ejecutables.														
3	CVE-2014-6287	94			2014-10-07	26/02/2021	10.0	Ninguno	Remoto	Bajo	No requerido	Completo	Completo	Completo

Figura 2.3.1 La principal Vulnerabilidad es la CVE-2014-6287

La función findMacroMarker en parserLib.pas en Rejetto HTTP File Server (aks HFS o HttpFileServer) 2.3x antes de 2.3c permite a atacantes remotos ejecutar programas arbitrarios a través de una secuencia% 00 en una acción de búsqueda.

Figura 2.3.2 CVE

Figura 2.3.2 Etapa de explotación > en esta se buscara atacar la vulnerabilidad principal por medio de las diferentes herramientas o comandos como:

- Nmap
- Metasploit
- netstat

A continuación, se describen los datos que fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina windows 7 X64.

Datos e información que ayudan a indentificar el fallo:

- Sistema operativo W7 el cual es un sistema que desde el 14 de Enero del 2020 no tiene actualizaciones de seguridad por parte del fabricante un riesgo alto a nivel del sistema
- Aplicación instalada Rejetto V 2.3 la cual según sea revisa es un software que presenta vulnerabilidades adicional que se usa como file server que como se entiende puede tener información relevante en una organización
- La aplicación al parecer tiene asociado un exploit que puede terminar en una Shell reversa y una sesión abierta de meterpreter.
- La aplicación en su vulnerabilidad tambien permite realizar escalamiento de privilegios por medio de la creación de un usuario tipo administrador del sistema

La herramienta que se utilizó para poder identificar los fallos de seguridad de la “máquina Windows 7? ¿Qué puerto abre la aplicación específica en el anexo?

Al tener acceso a la imagen de la maquina según entrega forense se inicia a validar directamente en la maquina

Figura 2.3.3 Hostname

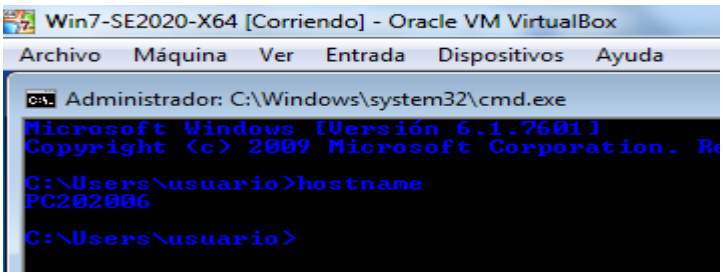


Figura 2.3.4 Direccion IP

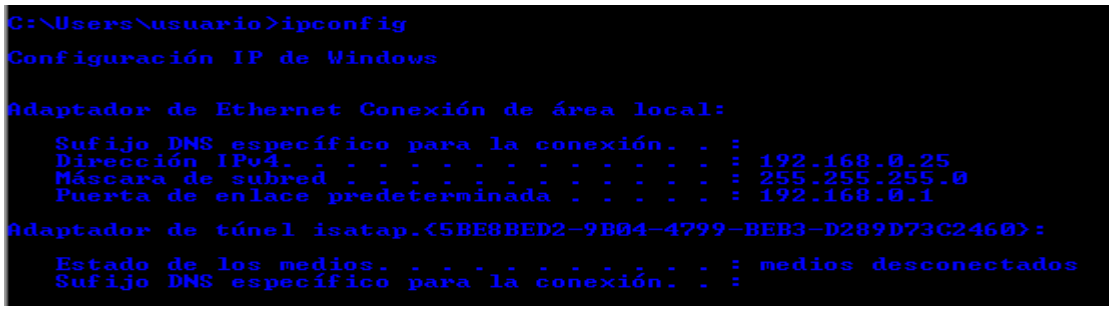


Figura 2.3.5 Puertos abiertos antes de ejecutar el programa

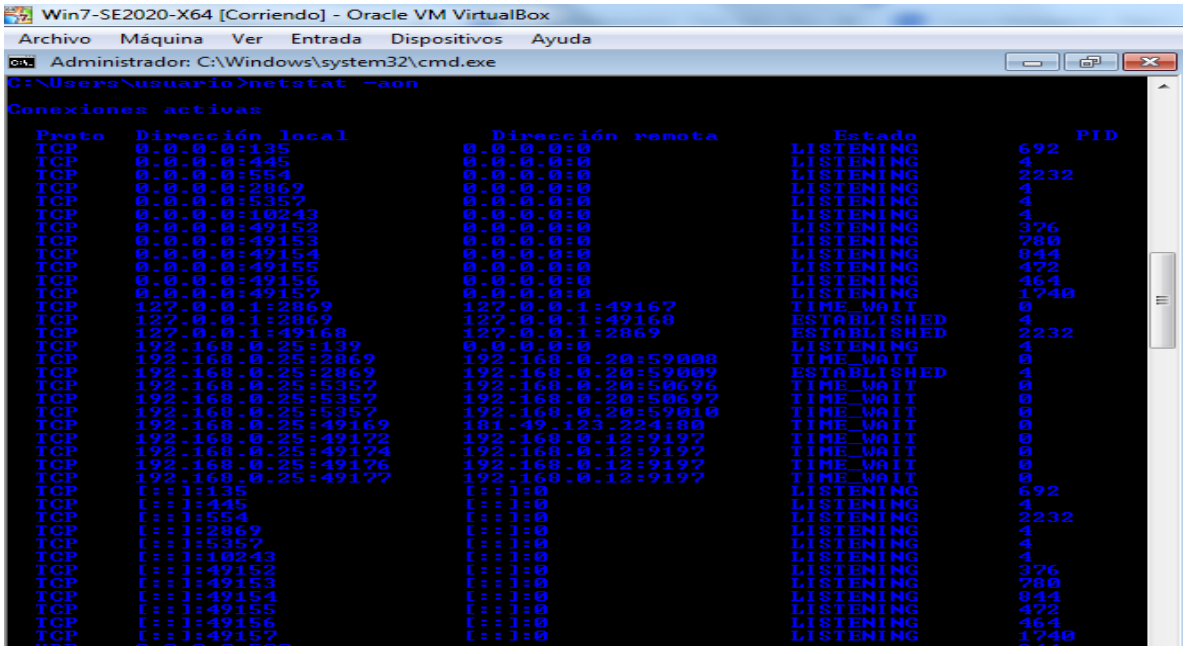


Figura 2.3.6 Puertos abiertos

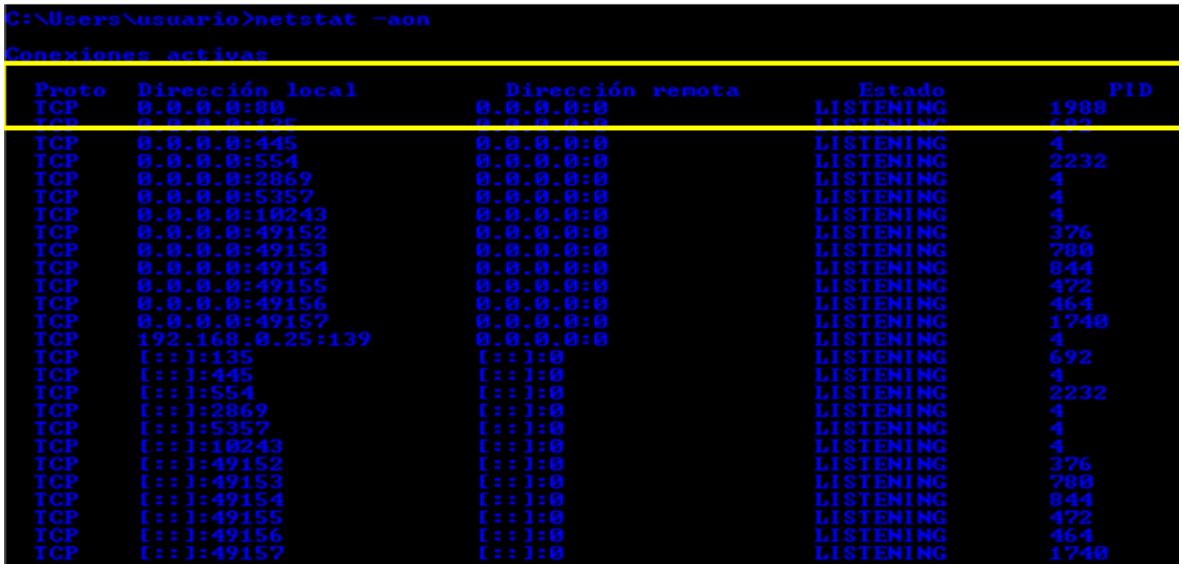
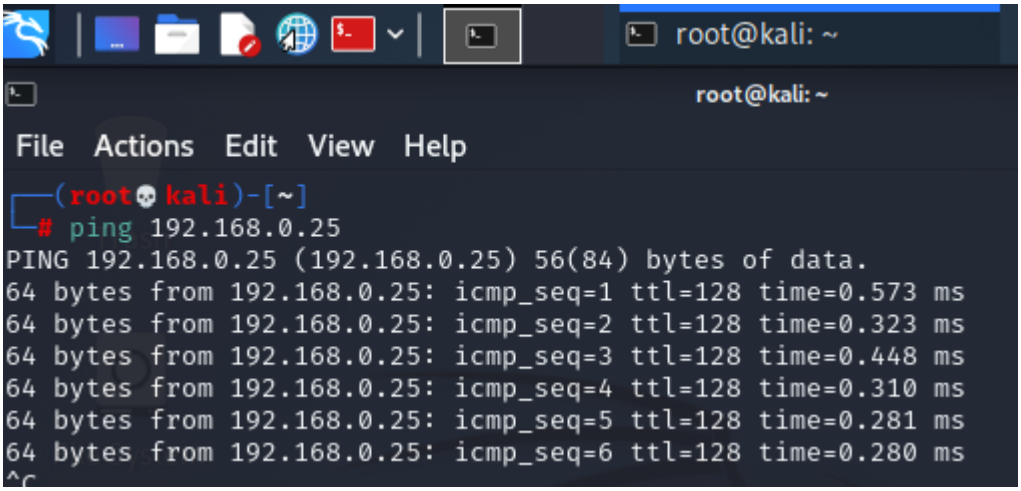


Figura 2.3.6 Puertos abiertos después de ejecutar y de estar activo el programa se encuentra que abre el puerto 80 al ser http

Figura 2.3.7 Ping y puerto



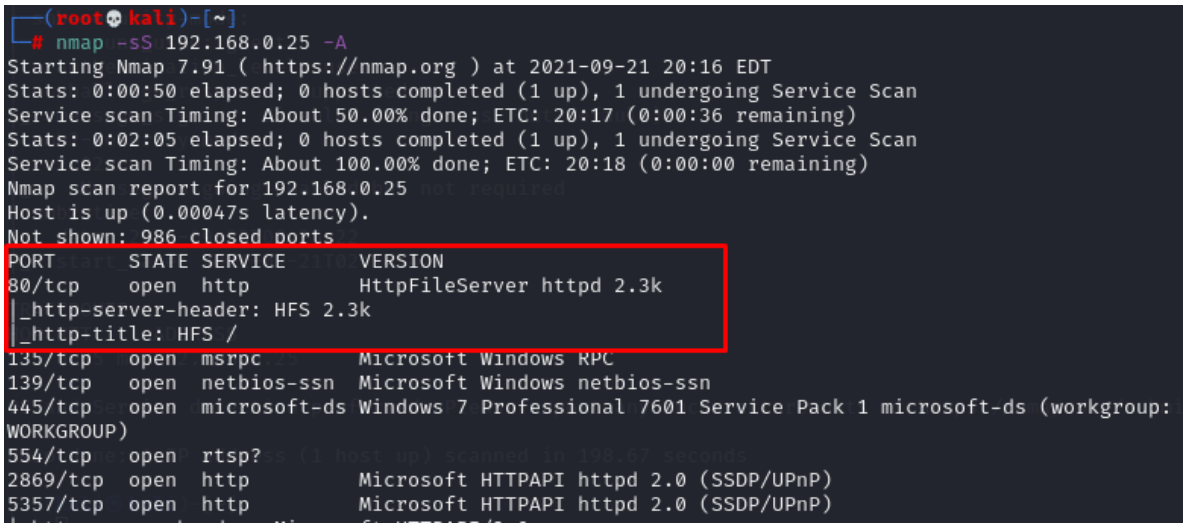


Figura 2.3.7 También se pueden detallar los puertos por medio del kali Linux como por ejemplo con nmap validando conectividad con esa maquina y encontrando que tiene instalado así como el sistema operativo del equipo a vulnerar.

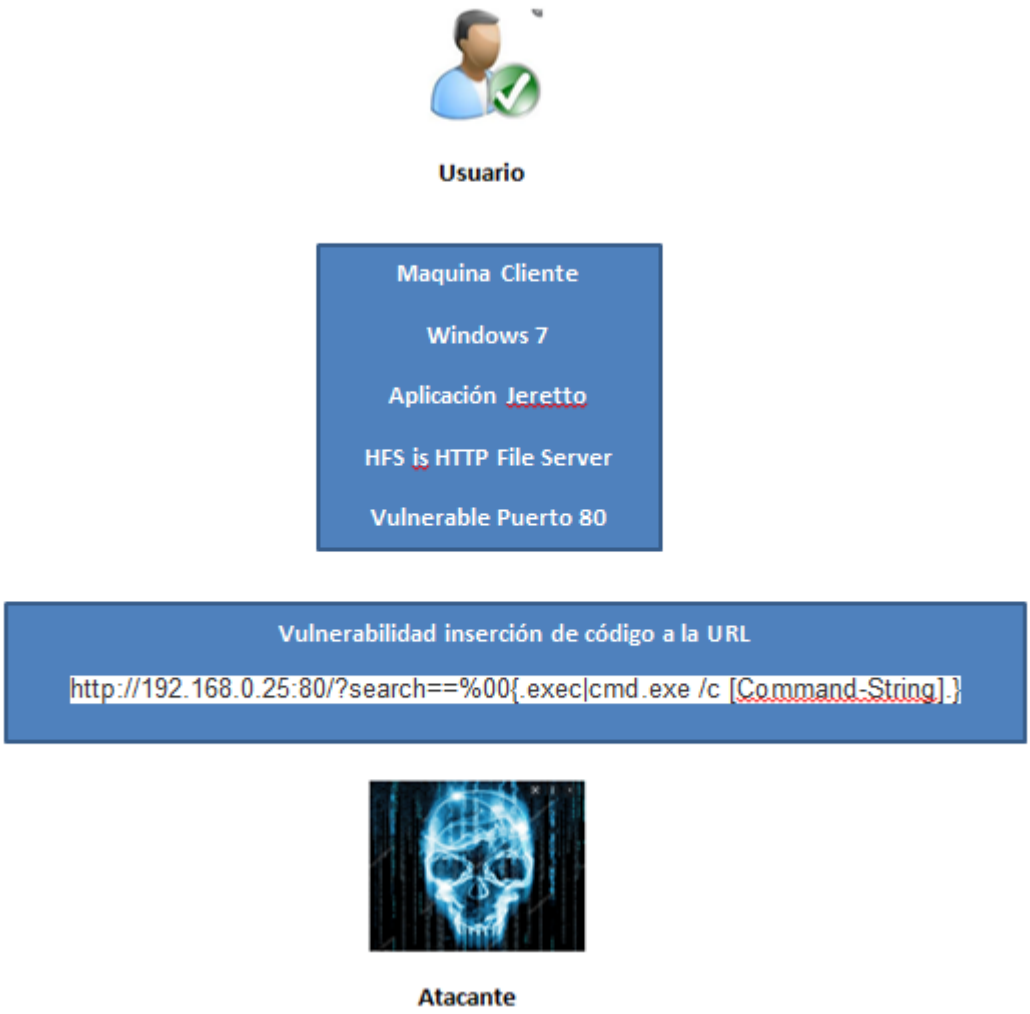
A continuación explico de manera específica cómo afecta el ataque a la máquina (Windows 7 X64), haga uso de gráficos para explicar el ataque.

Según la vulnerabilidad un equipo comprometido se puede reconocer por la versión de software, al conocer la vulnerabilidad que tiene la aplicación, y de no ser asegurada por medio de actualizaciones o parches se corre seriamente el riesgo de que sean atacadas.

El falla o vulnerabilidad conocido en la aplicación permite a un atacante remoto ejecutar código arbitrario en el sistema comprometido el cual aloja la aplicación. En este caso el equipo con dirección IP: 192.168.0.25. La función de comentario de archivo en Rejetto HTTP File Server (hfs) 2.3 y versiones anteriores permite a los atacantes remotos ejecutar código arbitrario cargando un archivo con ciertas secuencias de bytes UTF-8 no válidas que se interpretan como macro símbolos ejecutables por medio del puerto 80 y la url de acceso

En mas detalle la vulnerabilidad de seguridad en la función "findMacroMarker" en el archivo parserLib.pas en Rejetto HTTP File Server 2.3. La vulnerabilidad se debe al hecho de que el archivo parserLib.pas no maneja correctamente los bytes nulos. Un atacante remoto puede utilizar esta vulnerabilidad para ejecutar programas arbitrarios con la ayuda de la secuencia "% 00" en la operación de búsqueda como se observa en la imagen.

Figura 2.3.8 Esquema ataque



Documente cada uno de los pasos que ejecutó y sus respectivas evidencias para explotar la vulnerabilidad en la máquina Windows 7.

Sabiendo que el equipo cliente tiene una aplicación vulnerable como Rejetto y que al estar abierta esta aplicación muestra el puerto 80 abierto, se pretende entonces demostrar cómo se puede tener acceso a una Shell (cmd), de forma remota para poder controlar el equipo atacado. Iniciamos abriendo metasploit

Figura 2.3.9 Inicio Metasploit

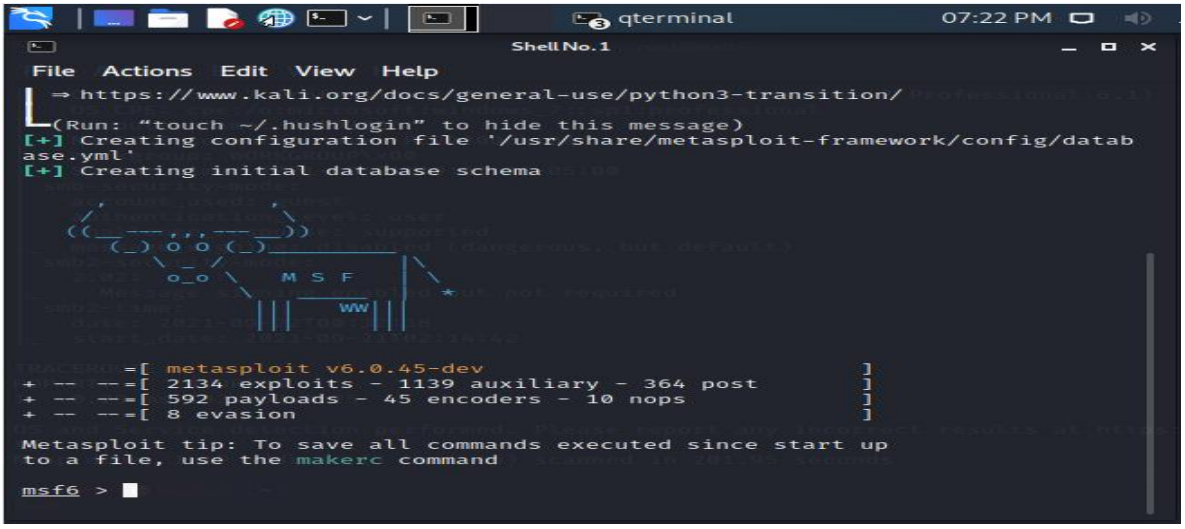


Figura 2.3.9 Lo planteado es poder tomar sesión en el equipo atacado por medio del rhost, o sea estar sobre la maquina victima como se observa en la imagen

Figura 2.3.10 Configuracion metasploit

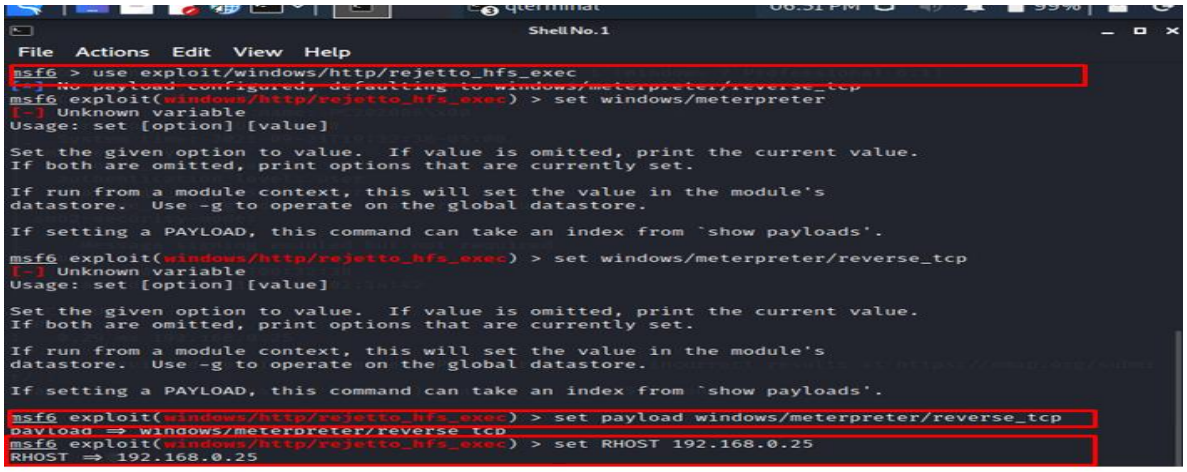


Figura 2.3.10 Ahora se va a ejecutar el exploit que hace referencia a esta vulnerabilidad sobre el equipo victima, el cual ingresa a la base de datos del metasploit que contiene los exploits de las vulnerabilidades ya conocidas, el exploit lo que realiza es una conexión reversa desde el equipo atacante, logrando una conexión o sesión en el host remoto.

Figura 2.3.11 Exploit

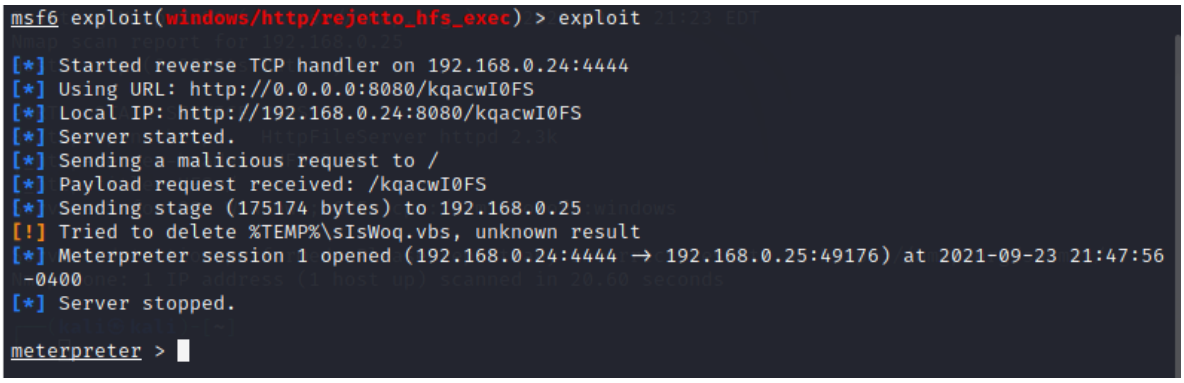


Figura 2.3.11 Ya teniendo una sesión sobre el equipo victima, se puede recolectar información que permite validar que se esta sobre el equipo victima por medio de comando Shell

Figura 2.3.12 Shell

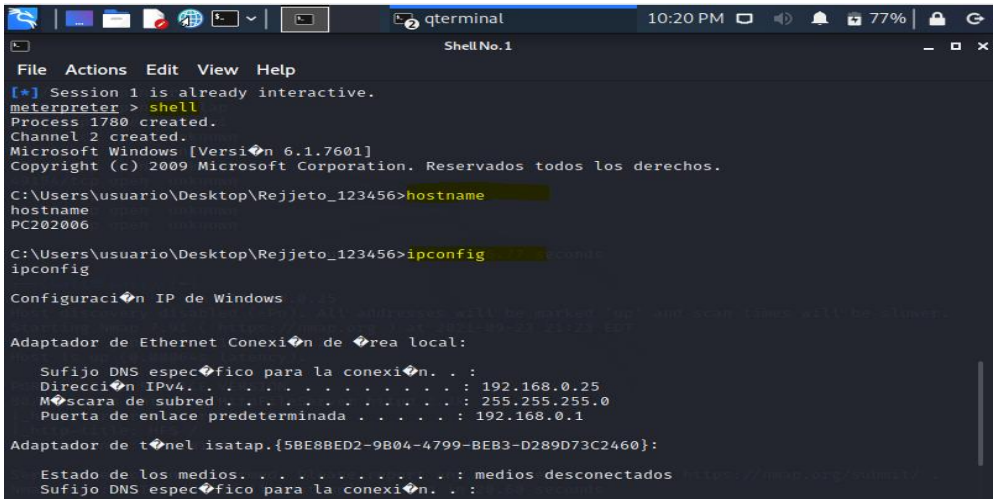


Figura 2.3.12 Como se logra evidenciar en este proceso por medio de la falla de seguridad en la aplicación sobre el sistema huésped se puede obtener y lograr fuga de información, todo por medio del puerto 80, esto evidencia que por Rejetto, se deja abierto el puerto, por el cual se puede realizar un ataque exitoso.

Figura 2.3.13 Creacion user

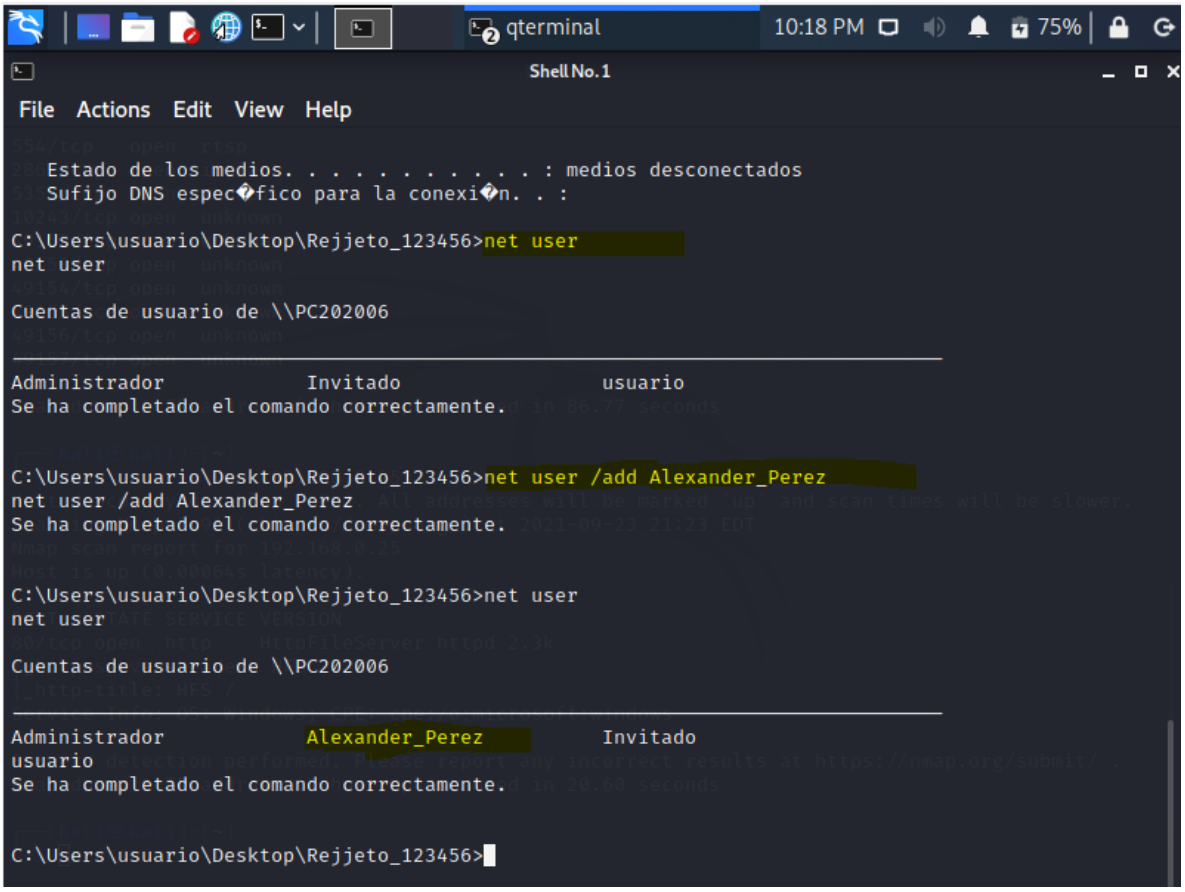


Figura 2.3.13 Para finalizar la revisión de la imagen del sistema y para demostrar a los directivos la falla de seguridad, se procede a crear un usuario por comando en este caso del especialista que esta revisando la imagen forense.

Nombre: Alexander
Apellido: Perez

2.4 Acciones de contención de ataques informáticos

Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real?

En un ambiente real no sé qué tan sencillo es identificar un ataque en tiempo real; para esto se tendría que tener en la red dispositivos o software de control como tipo (Network Access control, firewall con reglas detalladas de acceso y puertos específicos y documentados abiertos asi como software basado en inteligencia artificial que modele las amenazas y en tiempo real las reporte según aprendizaje y según conocimiento de la red.

Y en un escenario en el que se tengan los controles anteriores y se identifique el ataque en tiempo real los puntos que indagaría y acciones que realizaría serian de 2 tipos, acciones organizativas y acciones técnicas ya que un ataque o fuga de información puede afectar muchos frentes

Acciones organizativas

- Al encontrarse con un ataque en tiempo real lo 1ro a realizar seria información a las cabezas de la organización de un posible fuga o perdida de información; esto se debe realizar independiente del tipo de organización ya que se debe diseñar un plan de medidas al incidente y se debe identificar que temas legales o corporativos podrían quedar vulnerados. Adicional al informar tambien se debe tener claridad quien puede aprobar o tomar decisiones según corresponda.

Acciones técnicas

- Aunque suene muy rápido tomar esta acción lo 1ro que realizaría seria aislar la maquina vulnerada de la red ya sea aislando el segmento de red o la mejor forma es desconectándola de la red.
- Con el punto anterior cumplido y teniendo en cuenta que no hay software para este tipo de eventos ni presupuesto para adquisición según lo indica el anexo; iniciaría a revisar los eventos o logs de la maquina vulnerada para tener evidencia y saber que esta ocurriendo; como el escenario es de la actividad anterior vamos a revisar estos eventos sobre el equipo W7 con el software vulnerado.

Figura 2.4.1 Cuenta creada

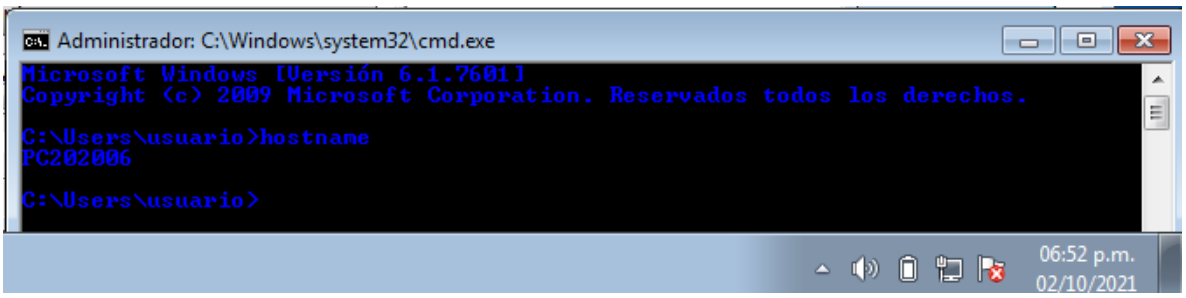


Figura 2.4.1 Se encuentran diferentes eventos de seguridad referentes a una creación de una cuenta de usuario local y a cambio de privilegios.

Figura 2.4.2 Eventos seguridad

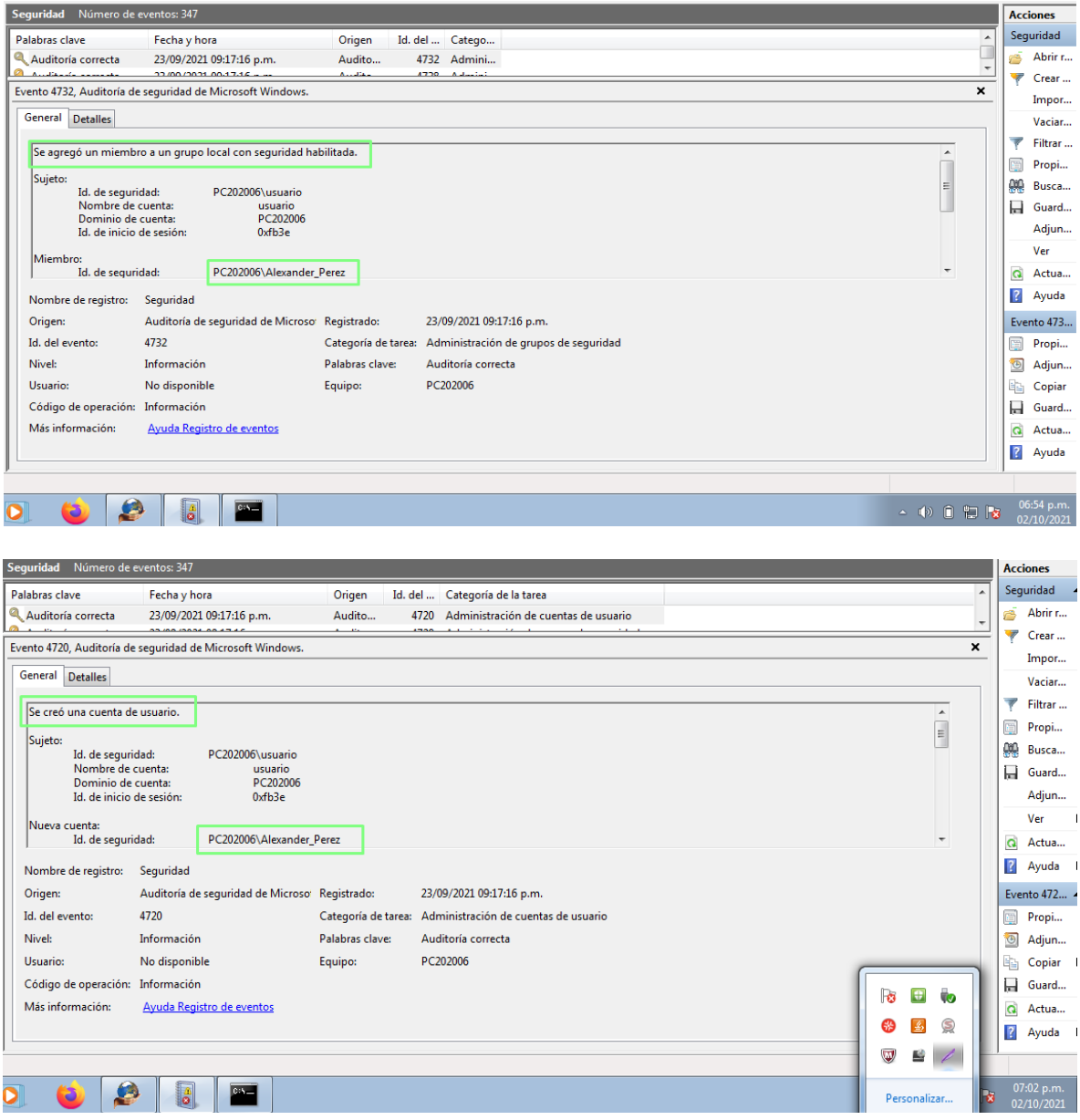


Figura 2.4.2 Que se identifica con las imágenes anteriores que fue creado y gestionado un usuario y según validación no fue creado por ninguno de los grupos de gestión operativa autorizados.

Figura 2.4.3 Conexiones

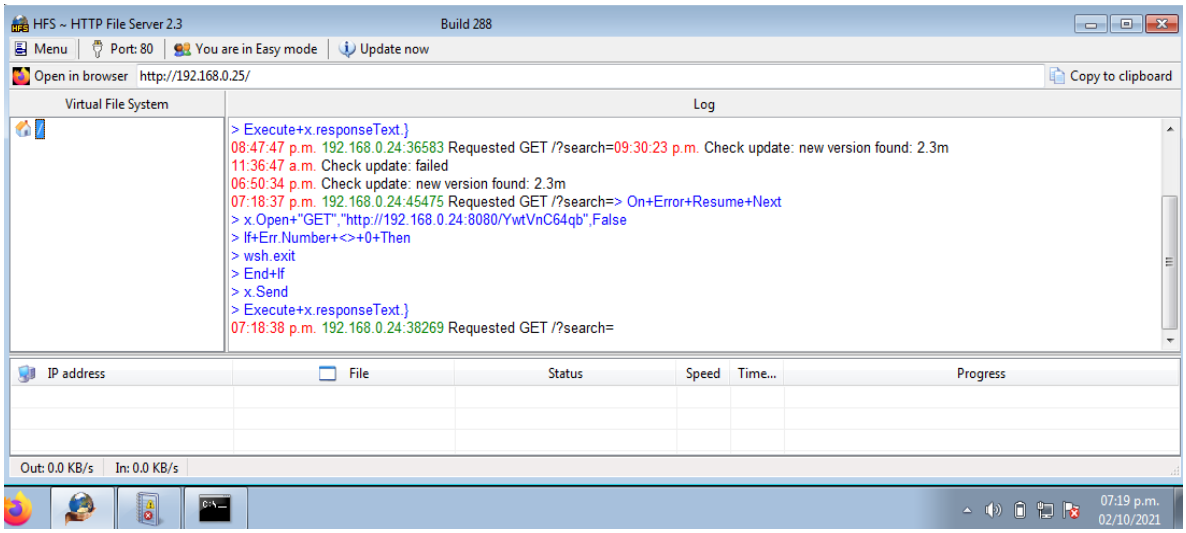
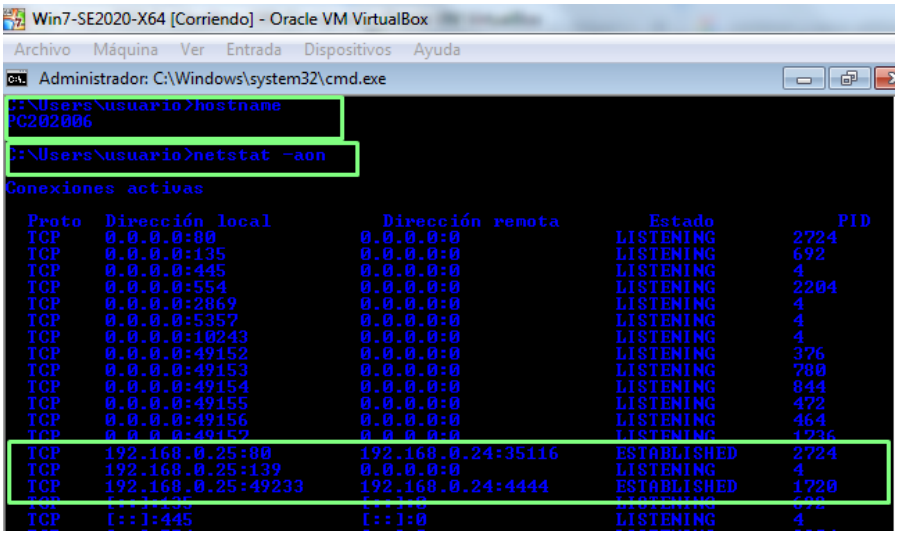


Figura 2.4.3 Otro de los puntos a revisar serían las diferentes conexiones que están establecidas y se puede realizar con un comando de sistema como **netstat** sobre la maquina vulnerada y conociendo que esta maquina tiene un software con una versión vulnerable

Se evidencia conexiones establecidas desde la maquina atacante hacia el equipo vulnerado por el puerto 80.

Figura 2.4.4 Conexiones establecidas



Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team qué medidas de hardenización propondría para que el ataque no se repita?

Las principales medidas que se deben tener para realizar hardening o aseguramiento a las maquinas y evitar que se repitan ataques serian los siguientes:

- Actualización de parches de seguridad de sistema operativo W7 hasta el último nivel y tener un plan de actualización según ciclo de Microsoft eso si este sistema operativo no estuviera fuera de soporte
- Subir firewall local del sistema dejando solo reglas específicas de entrada y salida de puertos según necesidad y según software instalado
- Monitoreo frecuente con reglas de la creación de usuarios locales y los privilegios asignados
- revisión de claves seguras, como política mínima de 12 caracteres alfanumérica con un diccionario configurado para evitar claves comunes
- Suspender servicios que no son necesarios en el sistema o que conllevan a tener aplicaciones propias de sistema ejecutándose en backlog
- Tener copias de respaldo a nivel de data de la aplicación y o el servicio a utilizar
- Pero creería que lo principal a optimizar seria actualizar como mínimo a W10 el sistema operativo y al igual seguir las recomendaciones anteriores
- Aunque los anteriores puntos hacen parte de lo que tiene que ver con el sistema también se debe tener claro y deben ser capacitados los usuarios en el uso de la información y de seguridad de la misma

Describa con sus palabras las diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos?

Las principales diferencias entre estos 2 equipos serían las siguientes:

- El equipo de respuesta a incidentes informáticos o CSIRT (Computer Security Incident Response Team) se enfoca inicialmente a ser entidades o grupos reactivos a responder ante ataques ya sucedidos. Entre las acciones que realiza el grupo CIRT están el análisis del malware, la investigación de los eventos de cómo se produjeron los ataques, también pueden colaborar a retornar el servicio o sistema que presento el ataque, y también puede gestionar las vulnerabilidades que se detectaron en el proceso del ataque. Su funcion principal es, por tanto, recibir, analizar y responder ante los incidentes recibidos desde las diferentes comunidades que colaboran con otros CSIRT o con empresas o personas que lo soliciten.

- El equipo de respuesta BlueTeam es por el contrario al equipo de respuesta a incidentes un grupo o área donde los ingenieros Blueteam buscan preveer o ser proactivos ya que se ha pasado del análisis y respuesta una vez se producía la incidencia, a un papel más preventivo y educativo; no sólo se limitan a crear anuncio de seguridad y gestionar los incidentes, sino que diseñan herramientas de seguridad que brindan y dan recomendaciones para prevenir ataques y ponen a disposición de las diferentes comunidades la información recogida para que otros puedan usarla y asi entender y reconocer como mitigar posibles futuros ataques.
- Tambien el grupo de Blueteam puede realizar o se enfoca en una inspección profunda referente a las medidas de seguridad estandarizadas en la infraestructura de red en una organización, se realiza una contencion de la seguridad de la información según hallazgos del Red Team, de una manera preventiva.

Si dentro de un equipo Blueteam le indican que debe trabajar con CIS "Center For Internet Security" usted lo utilizaría para qué fin?

Antes de indicar para que se utilizaría, se indica que el CIS (Center for Internet Security) son un conjunto de buenas prácticas o marcos de ciberseguridad para una variedad de sistemas y productos de TI. Estos marcos de referencia proporcionan las configuraciones para garantizar el cumplimiento de los estándares de ciberseguridad acordados por la industria, los marcos de referencia son desarrollados por CIS junto con comunidades de ingenieros expertos en ciberseguridad.

Los CIS ofrecen diferentes programas a las corporaciones o empresas para promover los procedimientos de ciberseguridad. Los controles CIS proporcionan a las organizaciones un conjunto de procedimientos para reforzar la ciberseguridad y responder a los incidentes. Consisten en acciones enfocadas para reducir el riesgo de amenazas cibernéticas y pasos para resolver incidentes de TI graves.

Utilizaria estas mejores practicas o marcos de referencia para:

- Fortalecer o robustecer el software de sistema operativo como por ejemplo Windows Server aseguramiento.
- Actualmente y por el auge de las migraciones y pasos a la nube de servicios utilizaría estas mejores practicas para configurar la infraestructura y los servicios en la nube más conocidos, asi como aseguramiento de los servicios en la nube de Amazon Web Services, Microsoft Azure, Oracle Cloud Infrastructure y Google Cloud Computing Platform. Se debe tener en cuenta que estos servicios en la nube deben cumplir con las regulaciones de los gobiernos y que mejor que tener estos marcos.

Explique y redacte las funciones y características principales de lo que es un SIEM.

El SIEM (Security Information and Event Management) o en español que significa Gestión de Eventos e Información de Seguridad, es un software o aplicativo que buscar realizar obtener y monitorear los diferentes logs de los dispositivos y elementos de seguridad.

Las principales características del SIEM son:

- Se encarga de analizar y estructurar los diferentes datos recopilados para tener una visión global los mismos a nivel de seguridad de elementos como los son Firewalls, IDS (Sistema de detección de intrusiones) , IPS (Sistema de prevención de intrusiones), Antimalware, WAF (Firewall de aplicaciones web), Firewall de base de datos, proxys, EDR (Endpoint Detection and Response).
- Dentro de sus características la aplicación trabaja con cantidades de datos elevadas, puede aplicar analítica integrada para detectar amenazas con precisión. Y también puede correlacionar actividades relacionadas para priorizar incidentes.

Defina por lo menos 3 herramientas de contención de ataques informáticos "hardware o software", recuerde que las herramientas de contención son diferentes a las herramientas de detección

Dentro de las herramientas de contención de ataques según revisión se pueden encontrar las siguientes:

- **Cisco FireSight:** escanea la actividad de la red con sensores de inteligencia artificial, cuya configuración es actualizada según aprendizaje de los sensores con las últimas alertas detectadas. Cisco FireSIGHT avisa del incidente a ISE que cambiará inmediatamente la política de acceso a la red del usuario y del dispositivo, marcándolos como "sospechosos". Este cambio en la política de acceso hará que el resto de soluciones de seguridad de la red configurados restrinjan o denieguen el acceso al usuario y su dispositivo.
- **Splunk:** es un software de seguridad de sistema informático completo que se utiliza para monitorear la seguridad de la red. La herramienta se utiliza tanto para realizar análisis de red en tiempo real como para búsquedas históricas de datos de amenazas. Esta es una herramienta fácil de usar que contiene una interfaz de usuario unificada para capturar, indexar y recopilar datos y generar alertas, informes, paneles y gráficos en tiempo real

- **Ossec IDS:** Es una de las herramientas con mejor calificacion open-source IDS ya que incluye herramientas para correlación de eventos, capacidades de monitoreo, análisis de vulnerabilidades, respuesta automática de amenazas como modulos adicionales de trabajo

3. CONCLUSIONES

Los temas referenciados respecto a configuración del banco de pruebas fueron satisfactorios y es el inicio del proceso, el tema es bastante interesante y son las bases para profundizar en un proceso más robusto y complejo.

El kali es un sistema que tiene aplicaciones muy utilizadas y que generan un desarrollo adicional en el proceso de aprendizaje.

También entiendo que la ley aún es muy lapsa y aun está abierta a consideraciones abiertas porque no se detallan los muchos escenarios que puede llegar a tener respecto a el trato de la información y sus derivados.

En este tipo de actividades en las cuales se ponen a prueba los conocimientos informáticos prácticos donde se busca hallar posibles vulnerabilidades, nos demuestra de una mejor forma como mitigar y evitar amenazas o ataques

Mediante este tipo de actividades se buscan formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI por medio de la práctica.

Es de vital importancia identificar las diferentes opciones que se tienen para contener un ataque y esto nos lleva a tomar medidas preventivas. También se logra tomar conciencia en un entorno laboral de las diferentes amenazas y los medios que se pueden utilizar para contener esas amenazas.

Como profesional crítico y analítico realizando la investigación de incidentes desarrollando la capacidad de identificar y entender la manera en la cual se ejecutan posibles delitos informáticos y como poder mitigarlos

En este tipo de actividades en las cuales se ponen a prueba los conocimientos informáticos prácticos donde se busca contener las amenazas y posibles vulnerabilidades, nos enseña a tomar experiencia y a saber cómo actuar en dado caso de tener que pasar por uno de estos eventos.

El trabajo planteado es óptimo para identificar, analizar y llegar a conclusiones lógicas dentro del proceso de contención.

REFERENCIAS BIBLIOGRAFICAS

Villanueva, Lina (2019) "en Colombia: agencias y complicidades mediáticas. [En línea], Recuperado de https://www.researchgate.net/profile/Lina-

Colombia. Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC (2009). Ley 1273 [LEY_1273_2009]. Mintic. (p. 1-4), [En línea], Recuperado de: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. (2018). Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

Pastor, Ricos Pentesting y generación de exploits con Metasploit. Recuperado de: https://repository.unad.edu.co/handle/10596/2129

Siem, (2020) [En línea], Recuperado de https://www.tuyu.es/soluciones-siem/

Jigsaw, (2021) [En línea], Recuperado de https://www.jigsawacademy.com/the-top-5-cyber-security-tools-used-by%20organizations/#Splunk

Avila, Gualdron. (2020), et al. Estudio de las mejores prácticas de Ethical Hacking, para generar un nuevo método que facilité la ejecución de análisis de seguridad enfocados a pruebas de penetración. Recuperado de: https://repository.unad.edu.co/handle/10596/21293

Offensive-security. Meterpreter Basic Commands. [En línea], Recuperado de: https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/

Sic, (2009) [En línea], Recuperado de: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Jelen, S. Cybersecurity Red Team Versus Blue Team - Main Differences Explained. [En línea], Recuperado de: https://securitytrails.com/blog/cybersecurity-red-blueteam

Nullsector. Explotar Vulnerabilidad EternalBlue con Metasploit. [En línea], Recuperado de: https://nullsector.co/explotar-vulnerabilidad-eternalblue-conmetasploit/

Tavakoli, O. How ready are you to stop an advanced attack? [En línea], Recuperado de: https://www.csoonline.com/article/3241889/how-ready-are-you-to-stop-anadvanced-attack.html

RepositoryUnad, (2021) [En línea], Recuperado de: https://repository.unad.edu.co/bitstream/handle/10596/40228/dcvillamild.pdf?sequence=1&isAllowed=y

Colombia. Código penal Colombiano (2000). Ley 599 [LEY_599_2000]. [En línea], Recuperado de: https://www.oas.org/dil/esp/Codigo_Penal_Colombia.pdf

Red Hat. El concepto de CVE. [En línea], Recuperado de: https://www.redhat.com/es/topics/security/what-is-cve

LINK VIDEO PRESENTACION

https://youtu.be/fOYrWGFLhsI